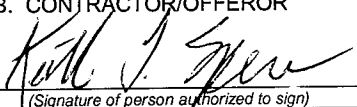
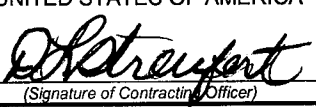


<b>AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT</b>		1. CONTRACT ID CODE <b>J</b>		PAGE OF PAGES <b>1 OF 6</b>
2. AMENDMENT/MODIFICATION NO. <b>P00049</b>		3. EFFECTIVE DATE <b>SEE BLOCK 16C.</b>		4. REQUISITION/PURCHASE REQ. NO.
6. ISSUED BY <b>SPACE AND NAVAL WARFARE SYSTEMS COMMAND CONTRACTING OFFICER: 02-N (DEBRA L STREUFERT) 2231 CRYSTAL DRIVE, SUITE 400 ARLINGTON, VA 22202-3721 PHONE: (703) 685-5508</b>		3. EFFECTIVE DATE <b>N00039</b>		5. PROJECT NO. (If applicable)
		7. ADMINISTERED BY (If other than Item 6) CODE		
8. NAME AND ADDRESS OF CONTRACTOR (No., street, country, State and ZIP Code)		(X)	9A. AMENDMENT OF SOLICITATION NO.	
<b>ELECTRONIC DATA SYSTEMS CORPORATION 13600 EDS DRIVE MS: A5S-B48 HERNDON, VA 20171 ATTN: NMCI CONTRACTS</b>			9B. DATED (SEE ITEM 11)	
		X	10A. MODIFICATION OF CONTRACT/ORDER NO. <b>N00024-00-D-6000</b>	
			10B. DATED (SEE ITEM 11) <b>06 OCTOBER 2000</b>	
CODE <b>1U305</b> FACILITY CODE				
<b>11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS</b>				
<input type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers <input type="checkbox"/> is extended <input type="checkbox"/> is not extended.				
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods:				
(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. <b>FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER.</b> If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.				
12. ACCOUNTING AND APPROPRIATION DATA (If required) <b>NOT APPLICABLE</b>				
<b>13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.</b>				
(X)	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.			
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).			
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: <b>FAR CLAUSE 52.212-4 (CHANGES)</b>			
	D. OTHER (Specify type of modification and authority)			
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input checked="" type="checkbox"/> is required to sign this document and return <u>ORIGINAL</u> copies to the issuing office.				
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)				
The purpose of this modification is to revise Attachment 7, DD Form 254 Contract Security Classification Specification, to incorporate Exhibit A, Requirements for Protection of Naval Nuclear Propulsion Information, attached hereto and made a part hereof. Additionally, the purpose of this modification is to address the specific requirements for the NNPI Community of Interest (COI), as set forth in this modification. All basic seat requirements set forth in this contract apply to this COI. As specified in Attachment 1 to the contract, section 4.11 (NMCI Enclaves) and Attachment 4 to the contract, section 1.2.1.9, a COI is defined as a logical grouping of users with access to information that should not be made available to the general user population. This modification identifies Contractor responsibilities for safeguarding data and Government responsibilities for safeguarding information.				
Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.				
15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)		
<b>KEITH SPENCER, NMCI CONTRACT MANAGER</b>		<b>DEBRA L. STREUFERT</b>		
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED	
 (Signature of person authorized to sign)	<b>12 Sep 2002</b>	BY  (Signature of Contracting Officer)	<b>12 Sept 02</b>	
NSN 7540-01-152-8070 PREVIOUS EDITION UNUSABLE		30-105		STANDARD FORM 30 (REV. 10-83) FAR (48 CFR) 53.243

## **Requirements for Protection of Naval Nuclear Propulsion Information**

### **1. General Protections**

- 1.1. Naval Nuclear Propulsion Information (NNPI) shall be safeguarded at all times on the NMCI. Safeguards shall be applied so that such information is accessed only by authorized individuals, is used only for its intended purpose, retains its content integrity, and is marked, handled, and disposed of properly, as required by NAVSEAINST C5511.32B.
- 1.2. The safeguarding of NNPI and NMCI resources (against sabotage, tampering, denial of services, espionage, fraud, misappropriation, misuses, or release to unauthorized persons) shall be accomplished through the continuous employment of safeguards consisting of administrative, procedural, physical and/or environmental, personnel, communications security, emanations security, and computer security (i.e. hardware, firmware and software), as required. The mix of safeguards selected shall achieve the requisite level of security or protection. The requisite safeguarding requirements are described in Attachment 4 to the basic contract.

### **2. Definitions**

- 2.1. Naval Nuclear Propulsion Information (NNPI) – Per NAVSEAINST C5511.32B: all information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of Naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities. NNPI may be unclassified (U-NNPI) or classified (C-NNPI). For this document, statements concerning “NNPI” shall apply equally and separately to both U-NNPI and C-NNPI.
- 2.2. U-NNPI Community of Interest (COI) – The group of unclassified NMCI users who are U.S. citizens and have a need to know U-NNPI.
- 2.3. C-NNPI COI – The group of SECRET NMCI users who are U.S. citizens, have final Government clearances of SECRET or higher, and have a need to know C-NNPI.
- 2.4. NNPI Community of Interest Officer (NNPI COIO) – Any activity that routinely deals with NNPI on NMCI shall designate an individual familiar with NNPI protection requirements as the NNPI COIO. Each activity shall ensure that the NNPI COIO is technically qualified, or that a technically qualified person shall be available for their consultation. The NNPI COIO’s primary responsibility shall be to ensure that only site personnel with a need-to-know are granted and allowed to retain access to the NNPI community of interest on the NMCI. If there is an NNPI Control Officer as defined by NAVSEAINST C5511.32B, that individual shall be or shall designate the site NNPI COIO.
- 2.5. NNPI Workspace – A physical area that is designated by the Government as a location for hardware that may process NNPI. An area shall be designated an NNPI workspace only if there are physical security measures in place to prevent unrestricted access to the area by non-U.S. citizens.

- 2.6. U-NNPI Hardware – Unclassified NMCI hardware (e.g., seats, servers, backup tapes, routers and printers) that is designated for storage or transmission of U-NNPI.
- 2.7. C-NNPI Hardware – SECRET NMCI hardware (e.g., seats, servers, backup tapes, routers and printers) that is designated for storage or transmission of C-NNPI.
3. The Contractor is responsible for the confidentiality, integrity, authenticity, identification, access control, non-repudiation, survivability and availability of Naval Nuclear Propulsion Information (NNPI) contained on the NMCI. The Contractor is not responsible for designating data as NNPI or disclosure of NNPI by authorized NNPI COI users.
4. The Contractor shall implement hardware and system configuration measures for protection of NNPI in such a manner that NMCI users may not compromise them.
5. Hardware
  - 5.1. The Contractor shall assume that all NNPI hardware actually stores NNPI.
  - 5.2. The Contractor shall store information identified by the Government as NNPI only on NNPI hardware.
  - 5.3. Labeling
    - 5.3.1. The Contractor shall label all user-accessible NNPI hardware as such. This includes seats (desktop and portable), printers and wall plugs.
    - 5.3.2. The Contractor shall ensure that notices are posted at the entries to server farms, identifying the potential presence of NNPI.
    - 5.3.3. It is not necessary to label equipment that transmits encrypted NNPI.
    - 5.3.4. These requirements satisfy the requirement of NAVSEAINST C5511.32B that ADP equipment will be marked to identify the highest level of information authorized.
  - 5.4. An NMCI seat designated as NNPI hardware shall not have a foreign national seat configuration (as described in the NMCI SSAA, Appendix P, Security Concept of Operations).
  - 5.5. NNPI hardware shall be located in a designated NNPI workspace. If non-U.S. citizen access to a NNPI workspace is required, the foreign national shall be escorted by a U.S. citizen, to prevent “unauthorized access to” of any NNPI (per NAVSEAINST C5511.32B).
6. Communities of interest
  - 6.1. There shall be a community of interest (COI) of users of U-NNPI on the unclassified NMCI.
    - 6.1.1. Users in the U-NNPI COI shall be limited to U.S. citizens.
    - 6.1.2. Users in the U-NNPI COI shall be limited to those unclassified NMCI users with a need to access U-NNPI, as determined by the site NNPI COIO.
    - 6.1.3. Users in the U-NNPI COI shall be identifiable in the unclassified NMCI global address list.
  - 6.2. There shall be a COI of users of C-NNPI on the SECRET NMCI.

- 6.2.1. Users in the C-NNPI COI shall be limited to U.S. citizens. The NNPI COIO will provide a list of authorized users to the Contractor.
- 6.2.2. Users in the C-NNPI COI shall be limited to those SECRET NMCI users with a need to access C-NNPI, as determined by the site NNPI COIO.
- 6.2.3. Users in the C-NNPI COI shall be limited to those with final Government clearances of SECRET or higher.
- 6.2.4. Users in the C-NNPI COI shall be identifiable in the SECRET NMCI global address list.

7. Access to NNPI

- 7.1. NNPI data on NMCI shall be accessible only by a member of the NNPI COI logged on an NMCI seat that is designated NNPI hardware. NNPI data includes data stored on shared file servers; web pages; applications; e-mail; temporary files; swap files; and memory files.
- 7.2. A member of the NNPI COI shall be able to log on to an NMCI seat designated for NNPI, shall be able to access NNPI, and shall be able to access other data and services on NMCI.
  - 7.2.1. When a member of the U-NNPI COI logs on to an unclassified NMCI seat that is U-NNPI hardware, there shall be a splash screen displayed:

"You are approved to process up to and including unclassified naval nuclear propulsion information (U-NNPI) on the NMCI.

U-NNPI is not for release to foreign nationals and has special handling requirements (NOFORN). U-NNPI is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with prior approval of the Chief of Naval Operations (Director, Naval Nuclear Propulsion, DIR NNP (N00N)). It is your responsibility to protect U-NNPI from disclosure to individuals without a need-to-know.

You are NOT approved to process classified information on this system."

- 7.2.2. When a member of the C-NNPI COI logs on to a SECRET NMCI seat that is C-NNPI hardware, there shall be a splash screen displayed:

"You are approved to process up to and including SECRET naval nuclear propulsion information (NNPI) on the NMCI.

NNPI is not for release to foreign nationals and has special handling requirements (NOFORN). NNPI is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with prior approval of the Chief of Naval Operations (Director, Naval Nuclear Propulsion, DIR NNP (N00N)). It is your responsibility to protect NNPI from disclosure to individuals without a need-to-know.

Access to RESTRICTED DATA (RD) NNPI requires FINAL Government clearance. It is your responsibility to protect RD NNPI from disclosure to individuals without a final clearance.”

- 7.2.3. Splash screens shall require user action to dismiss.
- 7.3. An NMCI user who is not a member of the NNPI COI shall be able to log on to an NMCI seat that is NNPI hardware, shall not be able to access NNPI, and shall be able to access other data and services on NMCI.
- 7.4. A member of the NNPI COI shall be able to log on to an NMCI seat not designated for NNPI, shall not be able to access NNPI, and shall be able to access other data and services on NMCI.
- 7.5. Content
  - 7.5.1. The Contractor shall develop and maintain information system architecture and procedures, by which the Government will mark, store, retrieve, transmit and output (e.g., hard copy or removable media) NNPI data in the NMCI. Government user failure to follow these procedures is outside the scope of Contractor control.
  - 7.5.2. All “generic” NMCI data and services shall be accessible from NMCI seats designated to process NNPI.
  - 7.5.3. E-mail
    - 7.5.3.1. Members of the NNPI COI shall not be permitted to provide read or proxy rights to their e-mail accounts to non-members of the NNPI COI.
    - 7.5.3.2. Members of the NNPI COI shall not be permitted to access e-mail marked to contain NNPI from a remote access NMCI seat unless that seat is designated NNPI hardware and is connected to the NMCI in an NNPI workspace.
- 8. Transmission
  - 8.1. Onsite transmission
    - 8.1.1. NNPI transmitted within an NNPI workspace does not require encryption provided the originating point, transmission lines, and ending point are capable of being visually monitored or protected in a manner that will allow detection of tampering.
    - 8.1.2. C-NNPI transmission onsite must be in accordance with the requirements of NSTISSI No. 7003, Protective Distribution Systems (PDS), dated 13 December 1996.
  - 8.2. Any NNPI transmitted offsite must be encrypted.
  - 8.3. Encryption
    - 8.3.1. Encryption of U-NNPI must be accomplished by a method that meets FIPS 140-1 or FIPS 140-2 requirements.
    - 8.3.2. Encryption of C-NNPI must be accomplished by a method that meets NSA Type 1 requirements.
- 9. Auditing - As a part of ongoing collection of security data, the Contractor shall continually monitor for suspicious activity associated with NNPI in accordance with

Attachment 4 to the basic contract. NAVSEA 08 will provide separately criteria for suspicious activity associated with NNPI.

10. Incident Response - If NNPI is stored on non-NNPI hardware, that hardware shall be immediately made inaccessible to anyone on the NMCI, except those involved in evaluating the incident. The hardware shall not be returned to service without the agreement of the NNPI COIO.
11. The Contractor shall document NMCI architecture, procedures, and test plans and results for protection of NNPI in appendices to the NMCI System Security Authorization Agreement (SSAA). One appendix shall address U-NNPI on the unclassified NMCI; the other appendix shall address C-NNPI on the SECRET NMCI.

A CONFORMED COPY OF REVISED CONTRACT IS MADE A PART OF THIS  
MODIFICATION AS A RESULT OF THE CHANGES OUTLINED HEREIN.

All other terms and conditions of Contract N00024-00-D-6000 remain unchanged and in full  
force and effect.